(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開平8－160856
(43)公開日　平成８年(1996)６月21日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０９Ｃ	1/00		7259－5Ｊ		
Ｈ０４Ｌ	9/00				
	9/10				
	9/12				
				Ｈ０４Ｌ　9/00　Ｚ	

審査請求　未請求　請求項の数19　ＯＬ　（全 11 頁）

(21)出願番号　特願平6－299940

(22)出願日　平成６年(1994)12月２日

(71)出願人　000004226
日本電信電話株式会社
東京都新宿区西新宿三丁目19番２号

(72)発明者　高嶋　洋一
東京都千代田区内幸町１丁目１番６号　日本電信電話株式会社内

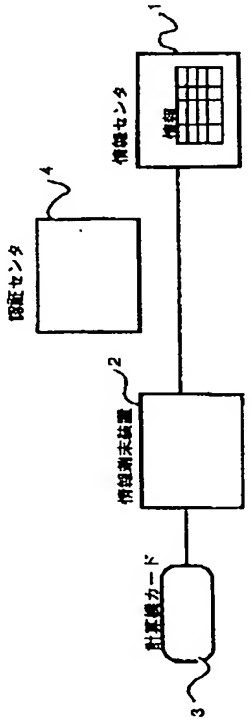
(72)発明者　石井　晋司
東京都千代田区内幸町１丁目１番６号　日本電信電話株式会社内

(72)発明者　山中　喜義
東京都千代田区内幸町１丁目１番６号　日本電信電話株式会社内

(74)代理人　弁理士　吉田　精孝

(54)【発明の名称】　ディジタル情報保護システム及びその方法

(57)【要約】
【目的】　情報が第３者に漏れることなく、正しい利用者であっても違法コピーが困難なディジタル情報保護システム及びその方法を提供する。
【構成】　情報端末装置２から利用者が選んだ利用情報の情報識別子を計算機カード３へ送って署名を受け、これを情報センタ１に送信し、情報センタ１では利用情報を暗号化するための鍵ＷＫを生成するとともに利用情報を該鍵ＷＫで暗号化して情報端末装置２に蓄積し、また、計算機カード３から利用情報が蓄積されたことを示す署名とともに配達証明のための乱数を情報センタ１に送り、情報センタ１で鍵ＷＫを前記乱数で変換して計算機カード３に配送し、計算機カード３から鍵ＷＫを情報端末装置２にセットした後、前記蓄積された利用情報を該セットされた鍵ＷＫで復号する。



【特許請求の範囲】

【請求項１】　共通鍵暗号方式もしくは公開鍵暗号方式の公開鍵により暗号化されたディジタル情報を情報センタから通信回線、無線、パッケージメディア等を介して情報端末装置に蓄積し、利用する前に計算機カード内に秘密の復号鍵ＷＫを情報センタから得て、利用する毎に計算機カード内の復号鍵ＷＫで情報端末装置に暗号化されて蓄積された情報を復号しつつ情報端末装置にて利用することを特徴とするディジタル情報保護システム。

【請求項２】　情報センタは、ディジタル情報を蓄積する情報蓄積手段と、情報端末装置との通信を行う通信制御手段と、情報暗号鍵及び復号鍵を生成する鍵生成手段と、ディジタル情報を暗号化する暗号化手段と、鍵を暗号通信するための公開鍵暗号化手段と、署名を行うための署名（公開鍵暗号復号）変換手段と、配達証明用の情報変換手段とを具備したことを特徴とする請求項１記載のディジタル情報保護システム。

【請求項３】　情報端末装置は、情報センタとの通信を行う通信制御手段と、計算機カードとの通信を行う通信制御手段と、ディジタル情報を蓄積する情報蓄積手段と、鍵を暗号通信するための公開鍵暗号化手段と、署名を行うための署名（公開鍵暗号復号）変換手段と、乱数を発生する乱数発生手段と、前記乱数と計算機カードから受信した乱数との値を照合する照合手段と、自装置の秘密鍵を格納する秘密鍵蓄積手段と、鍵情報及びディジタル情報を復号する復号手段と、前記乱数発生手段、照合手段、秘密鍵蓄積手段及び復号手段の機密を物理的に保護する機密保護手段とを具備したことを特徴とする請求項１記載のディジタル情報保護システム。

【請求項４】　計算機カードは、情報端末装置との通信を行う通信制御手段と、鍵を暗号通信するための公開鍵暗号化手段と、署名を行うための署名（公開鍵暗号復号）変換手段と、配達証明用の情報変換手段とを具備したことを特徴とする請求項１記載のディジタル情報保護システム。

【請求項５】　請求項２記載の情報センタと、請求項３記載の情報端末装置と、請求項４記載の計算機カードとを備えたことを特徴とする請求項１記載のディジタル情報保護システム。

【請求項６】　計算機カードと情報端末装置が相互に認証し、
計算機カードが利用者を確認し、
利用者の要求情報に署名してさらに暗号化して情報センタにアクセスし、
暗号化された利用情報を情報端末装置に蓄積し、蓄積されたことを示す受領署名を情報センタへ返送し、
利用情報を復号するための鍵ＷＫを利用の前に計算機カードに登録し、鍵ＷＫが配送されていることを配達証明によって保証し、
計算機カードから鍵ＷＫが情報端末装置にセットされた後、情報端末装置に蓄積された暗号化情報を情報端末装置で復号しながら、その情報を利用することと、要求情報と暗号化情報の受領署名と配達証明情報を課金根拠として記録することを特徴とするディジタル情報保護方法。

【請求項７】　計算機カードと情報端末装置が相互に認証する方法として、情報端末装置が生成した乱数を計算機カードに送り、計算機カードが署名暗号化したものを情報端末装置が受け取り、元の乱数と辻褄が合っているか否かをチェックすることを特徴とする請求項６記載のディジタル情報保護方法。

【請求項８】　計算機カードが情報端末装置を操作する利用者を認証する方法として、予め定めたパスワードを計算機カードに格納しておき、情報端末装置から入力された文字列が一致するかどうかをチェックし、入力誤りが所定の回数を越えた時はエラー処理し、該エラーが一定の回数続けて繰り返された場合は計算機カードを無効とするように制御することを特徴とする請求項６記載のディジタル情報保護方法。

【請求項９】　計算機カードが情報端末装置を操作する利用者を認証する方法として、予め定めたパスワードを計算機カードに暗号化して格納しておき、情報端末装置から入力された文字列が暗号化したものと一致するか否か（又は計算機カードに格納された暗号化されたパスワードを復号したものが情報端末装置から入力されたものと一致するか否か）をチェックすることを特徴とする請求項６記載のディジタル情報保護方法。

【請求項１０】　計算機カードが情報端末装置を操作する利用者を認証する方法として、予め定めたパスワードを計算機カードに暗号化して又はそのまま格納しておき、情報端末装置から入力された文字列を、情報端末装置と計算機カードとの間で暗号通信し、入力された文字列が暗号化したもの又はそのままのものと一致するか否かをチェックし、一致しているか否かによって生成した乱数のパリティを調節し、その乱数を暗号通信することを特徴とする請求項６記載のディジタル情報保護方法。

【請求項１１】　計算機カードが情報端末装置を操作する利用者を認証する方法として、予め定めたパスワードを計算機カードに暗号化して又はそのまま格納しておき、情報端末装置から入力された文字列に情報端末装置で生成した乱数を加えて（あるいは排他的論理和をとって）、情報端末装置と計算機カードとの間で暗号通信し、計算機カードで送られてきた文字列から予め登録してあるパスワードを引き（あるいは排他的論理和をとって）、得られた値を情報端末装置に返送し、情報端末装置で生成した乱数と返送された値とが一致するか否かでチェックすることを特徴とする請求項６記載のディジタル情報保護方法。

【請求項１２】　利用者が選んだ情報の情報識別子と情報センタの公開鍵とその証明書とを計算機カードへ送信

し、計算機カードが情報識別子に署名暗号化し、情報端末装置でそれに計算機カードの公開鍵とその証明書を付け加えて情報センタに送信することにより、情報センタへの不正アクセスを防止することを特徴とする請求項６記載のディジタル情報保護方法。

【請求項１３】　利用者が選んだ情報の情報識別子と情報センタの公開鍵とその証明書とを計算機カードへ送信し、計算機カードが情報識別子に署名したもの（ＲＱＳ）を暗号化し、情報端末装置でそれに計算機カードの公開鍵とその証明書を付け加えて情報センタに送信し、復号することによりＲＱＳを得て配達証明に利用することを特徴とする請求項６記載のディジタル情報保護方法。

【請求項１４】　利用情報を暗号化するための鍵ＷＫを情報センタが生成し、該鍵ＷＫで利用情報を暗号化し、暗号化情報に対してデータ圧縮等の適当なアルゴリズム（ハッシュアルゴリズム）を施した後、署名したものとともに情報端末装置へ送信し、暗号化情報は蓄積し、署名は計算機カードにて検証を行い、情報要求とともに暗号化情報が蓄積された情報端末装置の識別番号を計算機カード内へ登録することを特徴とする請求項６記載のディジタル情報保護方法。

【請求項１５】　計算機カードが暗号化情報にハッシュアルゴリズムを施した後に署名し、情報センタへ送り、情報センタがその署名を検証することによって暗号化情報が情報端末装置に正しく蓄積され、計算機カードにその情報識別子が登録されていることを確認することを特徴とする請求項６記載のディジタル情報保護方法。

【請求項１６】　情報センタと計算機カードとの間で鍵ＷＫが正しく配送されていることを保証する配達証明プロトコルを利用したことを特徴とする請求項６記載のディジタル情報保護方法。

【請求項１７】　計算機カードでＷＫ要求メッセージ内の乱数と鍵ＷＫを結合し、情報端末装置の公開鍵で暗号化して情報端末装置に送信し、情報端末装置でそれを復号した後、乱数が一致するか否かをチェックし、鍵ＷＫをセットし、蓄積された暗号化情報を復号することを特徴とする請求項６記載のディジタル情報保護方法。

【請求項１８】　一の情報端末装置に計算機カードを接続して購入した暗号化情報を、他の情報端末装置に前記計算機カードを接続して利用する場合、自動的に暗号化情報を一の情報端末装置から取り寄せて他の情報端末装置に蓄積することを特徴とする請求項６又は１４記載のディジタル情報保護方法。

【請求項１９】　一の情報端末装置に計算機カードを接続して購入した暗号化情報を、他の情報端末装置に前記計算機カードを接続して利用する場合、自動的に暗号化情報を一の情報端末装置から取り寄せて他の情報端末装置で復号しつつ利用することを特徴とする請求項６又は１４記載のディジタル情報保護方法。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、音楽、映像、プログラム等のディジタル情報の不正な複製を防止し得るディジタル情報保護システム及びその方法に関するものである。

【０００２】

【従来の技術】近年、音声・動画・静止画等のディジタル情報圧縮技術（例えば、ＭＰＥＧ＝Moving Picture Experts Group、ＪＰＥＧ＝Joint Photographic Coding Experts Group 等）及びＩＳＤＮを代表とする高速ディジタル通信技術の発達により、音楽・映像・絵画・書籍等の著作物をディジタル情報に変換し圧縮符号化して、情報センタ等から通信回線を介して各利用者端末へ配送することが可能となってきた。

【０００３】前述した映像等のディジタル情報に比べてデータ量の少ないコンピュータソフトウェアについては、既にパソコン通信等を利用して配送サービスを実施している例がある。また、最近、米国内においてサービスが開始されたＣＤ－ＲＯＭによるコンピュータソフトの販売方法では、暗号化された販売用ソフト及び暗号化されていないデモ用ソフトを格納したＣＤ－ＲＯＭを低価格で販売・配布し、デモ用ソフトを試用した利用者が購入希望を電話等でサービスセンタに申込むと、該利用者に復号鍵を通知して暗号化された販売用ソフトの使用を可能とする形式をとっている。

【０００４】

【発明が解決しようとする課題】前述した従来のパソコン通信等によるソフトウェアの販売方法の場合、ソフトウェアの暗号化がなされておらず、フロッピーディスク等のパッケージによるソフトウェアの販売方法に比べて、違法コピーをより容易にさせる環境を提供してしまうという問題があった。

【０００５】また、前述したＣＤ－ＲＯＭによるソフトウェアの販売方法の場合、電話等にて復号鍵をサービスセンタより受け取る際にセンタオペレーションを介在するため、人手がかかり、かつ利用者のプライバシーを保つことができないという問題があった。また、人手を介するため、復号鍵の横流し等の不正により違法コピーが可能になるという問題があった。

【０００６】本発明の目的は、情報が第３者に漏れることなく、正しい利用者であっても違法コピーが困難なディジタル情報保護システム及びその方法を提供することにある。

【０００７】

【課題を解決するための手段】本発明では前記目的を達成するため、物理的に封印された装置を情報端末装置に入れ、復号するための鍵ＷＫを計算機カードに蓄積し、利用した証拠として、要求情報、鍵受領署名、配達証明情報を情報センタが記録することを特徴とする。

【０００８】
【作用】本発明によれば、情報を暗号化して配送しているため、情報が第３者に漏れる恐れがなく、また、復号鍵が計算機カードの中に閉じ込められており、正しい利用者ですら復号鍵を知ることが困難であることと、情報端末装置に物理的に封印してある装置で鍵ＷＫの復号、情報の復号を行うため、違法コピーが困難であることと、配達証明情報により確実に課金を行えることから、情報提供者が安心して利用できるシステムとなる。
【０００９】
【実施例】図１は本発明のディジタル情報保護システムの一実施例を示すもので、図中、１は情報センタ、２は情報端末装置、３は計算機カード、４は認証センタである。
【００１０】情報センタ１は、情報提供者から供給された多数のディジタル情報を蓄積し、これをデータベースのように管理している。
【００１１】情報端末装置２は、ディジタル情報を利用するための画像表示装置、音声出力装置等を具備し、各利用者の家庭等に配置されている。情報センタ１と情報端末装置２とは通信ネットワークを通じて相互通信可能なように接続されている。
【００１２】計算機カード３は、情報端末装置２に対して着脱自在に取り付けられ、どの情報を購入したかという取り引き内容を示すデータを内部に蓄積しておくことができる。この計算機カード３は利用者毎に所持することができ、各利用者はこの計算機カード３を情報端末装置２に接続することによって、購入済のディジタル情報（画像、音楽等）を情報センタ１から情報端末装置２に送らせて利用することができる。
【００１３】なお、認証センタ４は公開鍵暗号方式を利用する際の準備段階でのみ必要となる。
【００１４】（情報センタの構成）図２は情報センタの詳細な構成を示すもので、図中、１１は利用情報を入力する情報入力部、１２は利用情報を蓄積する情報蓄積部、１３は利用情報を暗号化する情報暗号化部、１４は利用情報を暗号化する時に用いる鍵ＷＫを生成するＷＫ生成部、１５は鍵ＷＫを暗号化する公開変換部、１６は暗号化された鍵ＷＫが情報センタのものであることを示すための署名変換部、１７は情報センタの公開鍵やその認証センタによる証明書や演算の途中結果等を記憶するためのメモリ、１８は情報センタ全体の制御とハッシュアルゴリズムや配達証明のための情報変換等を実行するＣＰＵ、１９は計算機カードの公開鍵等を検証する公開鍵検証部、２０はネットワークとのやりとりを行うネットワーク入出力部である。
【００１５】（情報端末装置の構成）図３は情報端末装置の詳細な構成を示すもので、図中、２１は計算機カード３とのやりとりを行うカード入出力部、２２は公開鍵暗号の復号を行う復号鍵抽出部、２３は利用情報の復号を行う情報復号部、２４は復号された情報を出力する情報出力部、２５ａは画像表示装置、２５ｂは音声出力装置、２６は復号鍵抽出部２２、情報復号部２３及び情報出力部２４の機密を物理的に保護する機密保護手段、２７は利用情報を暗号化されたまま蓄積する情報蓄積部、２８はネットワークとのやりとりを行うネットワーク入出力部、２９は情報端末装置の公開鍵や認証センタの証明書や演算の途中結果等を記憶するためのメモリ、３０は情報端末装置全体の制御と乱数生成やハッシュアルゴリズムを実行するＣＰＵである。
【００１６】（計算機カードの構成）図４は計算機カードの詳細な構成を示すもので、図中、３１は認証センタの証明書で公開鍵が正当であることを検証する公開鍵検証装置、３２は暗号化や署名変換を施す公開鍵暗号装置、３３は情報端末装置２との通信を行う通信装置、３４は利用者認証のためのパスワード照合を行うパスワード照合装置、３５は購入情報の復号鍵を登録する復号鍵登録装置、３６は計算機カードの公開鍵やその証明書や演算途中結果を記憶するメモリ、３７は計算機カード全体の制御と乱数生成や配達証明のための情報変換等を行うＣＰＵ、３８は秘密鍵等の情報を保持するために必要な電圧監視装置、３９はバックアップ用の電池である。
【００１７】（情報利用プロトコル）
＜事前準備＞情報Ｍを鍵Ｋで暗号化して暗号化情報Ｃを得る変換をＣ＝ＥＫ（Ｍ）で表し、復号することをＭ＝ＤＫ（Ｃ）で表す。特に公開鍵暗号方式を利用する時は暗号化をＣ＝E_{KP}（Ｍ）、復号をＭ＝D_{KS}（Ｃ）で表す。後者は署名変換としても用いることがある。
【００１８】計算機カード３には予め識別子ＩＤＵと公開鍵ＫＰＵとその証明書ＸＰＵと認証センタ４の公開鍵ＫＰＣと秘密鍵ＫＳＵと秘密情報Ｓと公開情報ｎ’とが書き込まれており、特に秘密鍵ＫＳＵと秘密情報Ｓは読み出せないように保護されたエリアに書き込まれる。なお、ＩＤＵとＳとｎ’との間には$IDU=S^2 \bmod n'$の関係があり、ｎ’は２つの大きな素数の積で数百ビット程度の大きさである。証明書ＸＰＵは認証センタ４で公開鍵ＫＰＵを認証してもらい、ＸＰＵ＝D_{KSC}（ＸＰＵ）として求められる。但し、ＫＳＣは認証センタ４の秘密鍵で、これは認証センタ４以外には秘密にされる。
【００１９】同様に、情報端末装置２には予め識別子ＩＤＳと公開鍵ＫＰＳとその証明書ＸＰＳと認証センタ４の公開鍵ＫＰＣと秘密鍵ＫＳＳとが書き込まれ、情報センタ１には予め識別子ＩＤＭと公開鍵ＫＰＭとその証明書ＸＰＭと認証センタ４の公開鍵ＫＰＣと秘密鍵ＫＳＭとが書き込まれる。また、計算機カード３には利用者を認証するための情報（例えばパスワード）が読み出されないように登録される。
【００２０】＜計算機カード・情報端末相互認証＞図５は計算機カード・情報端末相互認証の工程を示すものである。

【００２１】計算機カード３が情報端末装置２に接続されると、情報端末装置２から、乱数Ｒと該情報端末装置２の公開鍵KPSとその公開鍵の証明書XPSと該情報端末装置２の識別子ＩDSとが計算機カード３へ送られる。

【００２２】計算機カード３はその内部に保持している認証センタ４の公開鍵KPCを利用して、情報端末装置２の公開鍵KPSとその証明書XPSとの辻褄が合っているか否かを確認することにより、情報端末装置２の公開鍵KPSが正当であるか否かを判断する。正当と判断された時は送られて来た乱数Ｒに署名暗号化変換を施し、Ｔ＝EK_{PS}（DK_{SU}（Ｒ））（又はDK_{SU}（EK_{PS}（Ｒ））なるＴと計算機カード３の公開鍵KPUとその証明書XPUと識別子ＩDUとを情報端末装置２に送信する。

【００２３】情報端末装置２はその内部に保持している認証センタ４の公開鍵KPCを利用して計算機カード３の公開鍵KPUが正当であることを確認した後、送られてきたＴと送ったＲとの辻褄が合っているか否かを確認することにより、相手が正しい計算機カードＩDUであるか否かを判断する。

【００２４】＜利用者認証＞図６は利用者認証の工程を示すものである。

【００２５】利用者は、情報端末装置２に予め計算機カード３に登録してあるパスワードを入力する。情報端末装置２は入力されたパスワードを計算機カード３に送信し、正しいかどうかを判断してもらう。パスワードの入力が正しい場合には、正当な利用者であると判断し、メニュー情報を利用者に示す。

【００２６】この際、パスワードの入力誤りは予め定めた所定の回数、例えば３回まで許容し、３回を越えた時はエラー処理、つまり正当な利用者でない可能性があるとして計算機カード３を排出し、さらに該エラーが予め定めた一定の回数、例えば５回続けて繰り返されたような場合は正当な利用者でないとして該カードを無効とする。

【００２７】なお、利用者認証の別の方法として、予め定めたパスワードを計算機カードに暗号化して格納しておき、情報端末装置から入力された文字列が暗号化したものと一致するか否か（又は計算機カードに格納された暗号化されたパスワードを復号したものが情報端末装置から入力されたものと一致するか否か）をチェックする方法、予め定めたパスワードを計算機カードに暗号化して又はそのまま格納しておき、情報端末装置から入力された文字列を、情報端末装置と計算機カードとの間で暗号通信し、入力された文字列が暗号化したもの又はそのままのものと一致するか否かをチェックし、一致しているか否かによって生成した乱数のパリティを調節し、その乱数を暗号通信する方法、予め定めたパスワードを計算機カードに暗号化して又はそのまま格納しておき、情報端末装置から入力された文字列に情報端末装置で生成した乱数を加えて（あるいは排他的論理和をとって）、情報端末装置と計算機カードとの間で暗号通信し、計算機カードで送られてきた文字列から予め登録してあるパスワードを引き（あるいは排他的論理和をとって）、得られた値を情報端末装置に返送し、情報端末装置で生成した乱数と返送された値とが一致するか否かでチェックする方法等が適用できる。

【００２８】＜利用者選択＞図７は利用者選択の工程を示すもので、利用者はメニュー情報から必要な情報を選ぶ。

【００２９】＜情報要求＞図８は情報を要求するための情報要求の工程を示すものである。

【００３０】利用者は選んだ情報の情報識別子Ｒeq（音楽情報の場合、国際レコーディングコード（ＩＳＲＣ）等の全世界共通コードや、情報提供業者が独自に付与した情報を一意に特定できる番号等）と情報センタ１の公開鍵KPMとその証明書XPMとを計算機カード３へ送信する。

【００３１】計算機カード３は認証センタ４の公開鍵KPCで情報センタ１の公開鍵KPMとその証明書XPMとの辻褄が合っていることを確認し、Reqに署名して、ＲＱＳ＝DK_{SU}（Req）なるＲＱＳを得る。これを情報センタ１の公開鍵KPMで暗号化し、RU＝EK_{PM}（ＲＱＳ）なるRUを情報端末装置２に送信する。

【００３２】情報端末装置２はRUを受けとると、それに計算機カード３の公開鍵KPUとその証明書XPUとを付け加えて情報センタ１に送信する。

【００３３】情報センタ１は送られてきた計算機カード３の公開鍵KPUとその証明書XPUとの辻褄が合っていることを確認し、RUからＲＱＳをＲＱＳ＝DK_{SM}（RU）として求め、さらにReqをReq＝EK_{PU}（ＲＱＳ）として求め、情報を検索する。

【００３４】＜情報配送・蓄積・情報センタ認証＞図９は情報配送・蓄積・情報センタ認証の工程を示すものである。

【００３５】利用情報Ｉを暗号化するための鍵ＷＫを情報センタ１が生成し、情報ＩをＣ＝EWK（Ｉ）として暗号化し、情報端末装置２の情報蓄積部に暗号化されたまま蓄積する。暗号化情報Ｃが確かに情報センタ１から送り出されたものであることを示すためには、これに情報センタ１の署名を付ける。なお、ここで、暗号化された情報全体に署名を付けることは効率的でないので、ある一方向性ハッシュアルゴリズムｈによってＣの量を削減したものｈ（Ｃ）に対してＳＩＭ＝DK_{SM}（ｈ（Ｃ））として署名を付ける。

【００３６】情報端末装置２は受けとった暗号化情報Ｃにハッシュアルゴリズムを施し、受けとったＳＩＭと一緒に計算機カード３へ送信する。

【００３７】計算機カード３はその署名が正しいかどうかを、情報センタ１の公開鍵KPMを用いてEK_{PM}（ＳＩＭ）がｈ（Ｃ）と一致するか否かで検証し、要求情報Ｒe

q、暗号化された情報端末装置２の識別番号ＩＤSを登録する。

【００３８】＜署名・配達証明準備＞図１０は署名・配達証明準備の工程を示すものである。

【００３９】計算機カード３は暗号化された情報Ｃが情報端末装置２に蓄積されたことを情報センタ１に知らせるため、ハッシュ化された暗号化情報ｈ（Ｃ）に計算機カード３の秘密鍵KSUで署名をし、SU＝DK_{SU}（ｈ（Ｃ））なるSUを送信する。

【００４０】情報センタ１はSUが正しいものであるかどうかを、EK_{PU}（SU）がｈ（Ｃ）と一致するか否かで検証する。

【００４１】次に、配達証明のために、乱数r_i（ｉ＝０，１，……，ｔ－１）を生成し、Xi＝$IDU^{ri} \bmod n'$によりXiを求め、ＸＸ＝（X0｜X1｜…｜Xt-1）を情報端末装置２を経由して情報センタ１へ送信する。但し、ｔは鍵WKのビット数で、｜は結合を意味する。

【００４２】＜鍵配送・配達証明＞図１１は鍵配送・配達証明の工程を示すものである。

【００４３】情報センタ１はＸＸとＲＱＳとWKからＥＥ＝WK‖ｈ（ＸＸ，ＲＱＳ）を求める。但し、‖はビット毎の排他的論理和を表すものとする。ＥＥを１ビットずつに分割し、それをe_i（ｉ＝０，１，……，ｔ－１）とする。

【００４４】まず、e_0を計算機カード３に送る。計算機カード３では受けとったe_0に対して、Y0＝$S^{(r_0+e_0)} \bmod n'$を計算し、Y0を情報センタ１へ送り返す。この時、ＩDU＝$S^2 \bmod n'$が成り立つようにＳが定められている。

【００４５】Y0を受けとった情報センタ１は$Y0^2 \equiv IDU^{e0} \cdot X0 \pmod{n'}$が成り立っているか否かを検証する。成り立っている場合は続けてe_1を送り、同様にY1を受けとって検証する。これをｔ回繰り返す。ｔ回繰り返された後、情報センタ１はRU，SU，e_i，Yi（ｉ＝０，１，……，ｔ－１）を、課金根拠として記録する。

【００４６】計算機カード３は、送られてきたe_iを結合してＥＥを求め、WK＝ＥＥ‖ｈ（ＸＸ，ＲＱＳ）によって、WKを得て、Req，ＩDSと組になるよう登録する。

【００４７】なお、ここではe_iの送り方を簡単にするため、１ビットずつにする方法を述べたが、何ビットかまとめて送る方法もあることはいうまでもない。

【００４８】＜情報利用＞図１２は情報利用の工程を示すものである。

【００４９】利用者が情報を利用する時は、計算機カード３を情報端末装置２に接続して該情報端末装置２を操作する。情報端末装置２から、乱数ｒを含んだWK要求メッセージReqWが計算機カード３へ送信される。計算機カード３ではReqW内の乱数ｒと鍵WKを結合し、それを情報端末装置２の公開鍵KPSで暗号化し、Ｖ＝EKPS（WK，ｒ）なるＶを情報端末装置２に送る。

【００５０】情報端末装置２ではＶをKSSを用いて復号した後、ｒが一致するか否かをチェックし、鍵WKをセットし、蓄積された暗号化情報Ｃを復号し、利用できるようにする。

【００５１】なお、KSSを用いて復号する装置からWKで復号する装置までは物理的に機密保持がなされている。その実現方法としては該当部分を頑丈な容器に入れ、封印をするか、R.Mori and M.Kawahara 'Superdistribution: The Concept and theArchitecture' Trans. IEICE, E-73, No.7, 1990-7に記載された方法を適用することが可能である。

【００５２】正当な利用者は、正しい計算機カード３を持っている限り、情報端末装置２に蓄積された情報を何回でも利用することができる。

【００５３】＜情報端末装置に情報が蓄積されていない場合の情報利用＞図１３は情報端末装置に情報が蓄積されていない場合の情報利用の工程を示すものである。

【００５４】図８と同様に情報要求がなされた後、計算機カード３ではその情報要求Reqが登録されているかをチェックし、登録されているならＩD'Sを情報端末装置ＩDSに返送する。情報端末装置ＩDSは別の情報端末装置ＩD'Sから暗号化情報Ｃを転送してもらい、図１２による情報利用で情報を利用する。

【００５５】また、転送してもらいつつ情報を利用する方法として、以下の方法がある。情報端末装置２はSUを情報センタ１へ送り出した後、計算機カード３内へ乱数ｒを含んだWK要求メッセージReqWを送信し、計算機カード３でReqW内の乱数ｒと鍵WKを結合し、それを情報端末装置２の公開鍵KPSで暗号化し、Ｖ＝EK_{PS}（WK，ｒ）なるＶを情報端末装置２に送信する。

【００５６】情報端末装置２ではＶをKSSを用いて復号した後、乱数ｒが一致するか否かをチェックし、鍵WKをセットする。暗号化情報Ｃを復号し、利用できるようにし、受けとったことを示すためにＡＣＫを返送する。この際、復号しながら蓄積するということも可能である。

【００５７】なお、前記実施例ではＩＳＤＮ等の公衆通信回線を利用する場合について示したが、専用線等のコネクションレスの回線にも適用できることはいうまでもない。

【００５８】

【発明の効果】以上説明したように本発明によれば、情報が第３者に漏れることがないことと、違法コピーが困難であり、さらに配達証明情報により確実に課金を行えることから、情報提供者が安心して利用できるシステムを構成でき、しかも利用者にとって不利になることはなく、利用したい情報が近くの情報端末装置に無くとも、情報センタへアクセスすることにより利用でき、また、

どの情報端末装置からでも利用可能となる等の利点がある。

【００５９】なお、本発明は、コンピュータソフトウェアのみならず、全ての暗号化ディジタル情報の通信利用による配送の際に適用できることは言うまでもない。

【図面の簡単な説明】

【図１】本発明のディジタル情報保護システムの一実施例を示す図

【図２】情報センタの詳細な構成図

【図３】情報端末装置の詳細な構成図

【図４】計算機カードの詳細な構成図

【図５】計算機カード・情報端末相互認証の工程を示す図

【図６】利用者認証の工程を示す図

【図７】利用者選択の工程を示す図

【図８】情報を要求するための情報要求の工程を示す図

【図９】情報配送・蓄積・情報センタ認証の工程を示す図

【図１０】署名・配達証明準備の工程を示す図

【図１１】鍵配送・配達証明の工程を示す図

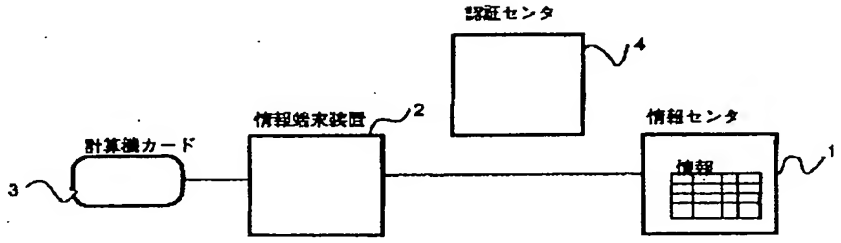
【図１２】情報利用の工程を示す図

【図１３】情報端末装置に情報が蓄積されていない場合の情報利用の工程を示す図

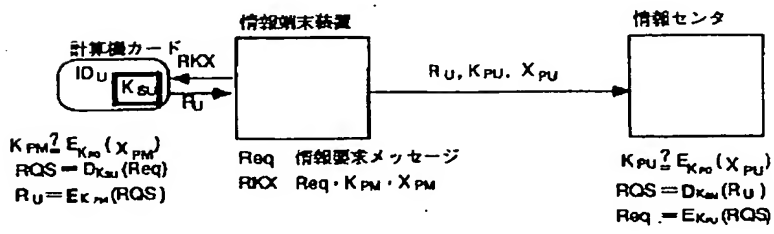
【符号の説明】

１…情報センタ、２…情報端末装置、３…計算機カード、１１…情報入力部、１２…情報蓄積部、１３…情報暗号化部、１４…ＷＫ生成部、１５…公開変換部、１６…署名変換部、１７…メモリ、１８…ＣＰＵ、１９…公開鍵検証部、２０…ネットワーク入出力部、２１…カード入出力部、２２…復号鍵抽出部、２３…情報復号部、２４…情報出力部、２５ａ…画像表示装置、２５ｂ…音声出力装置、２６…機密保護手段、２７…情報蓄積部、２８…ネットワーク入出力部、２９…メモリ、３０…ＣＰＵ、３１…公開鍵検証装置、３２…公開鍵暗号装置、３３…通信装置、３４…パスワード照合装置、３５…復号鍵登録装置、３６…メモリ、３７…ＣＰＵ、３８…電圧監視装置、３９…電池。

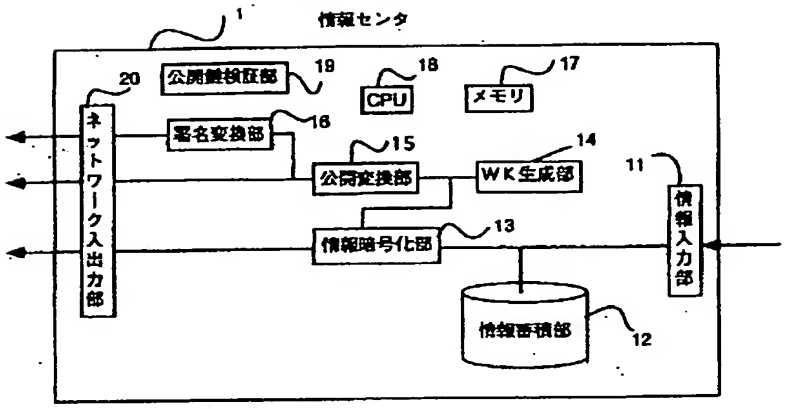
【図１】



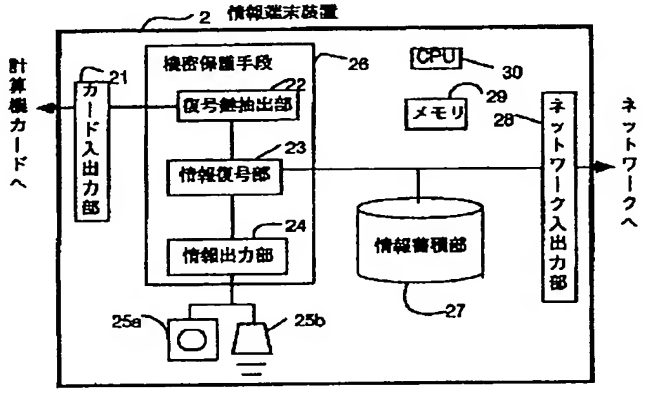
【図８】



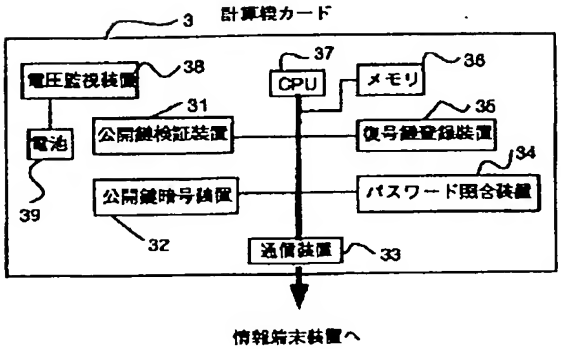
【図２】


1
情報センタ
20
ネットワーク入出力部
公開鍵検証部
19
CPU
18
メモリ
17
署名変換部
16
公開変換部
15
WK生成部
14
情報暗号化部
13
情報入力部
11
情報蓄積部
12

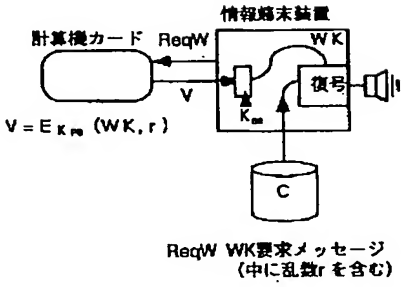
【図３】


2
情報端末装置
計算機カードへ
カード入出力部
21
機密保護手段
22
復号鍵抽出部
情報復号部
23
情報出力部
24
26
CPU
30
メモリ
29
28
ネットワーク入出力部
ネットワークへ
情報蓄積部
27
25a
25b

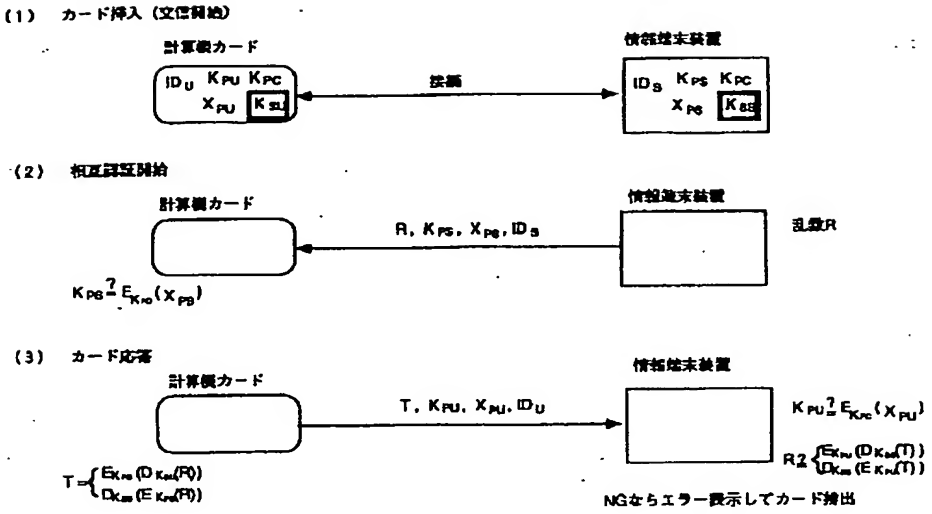
【図４】


3
計算機カード
電圧監視装置
38
CPU
37
メモリ
36
電池
39
公開鍵検証装置
31
復号鍵登録装置
35
公開鍵暗号装置
32
パスワード照合装置
34
通信装置
33
情報端末装置へ

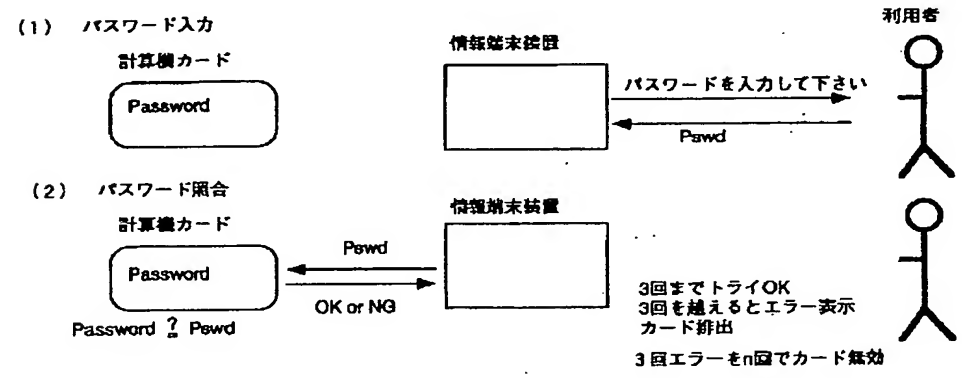
【図１２】


情報端末装置
計算機カード
ReqW
WK
V
復号
$V = E_{K_{PR}}(WK, r)$
K_{PR}
C
ReqW WK要求メッセージ
(中に乱数r を含む)

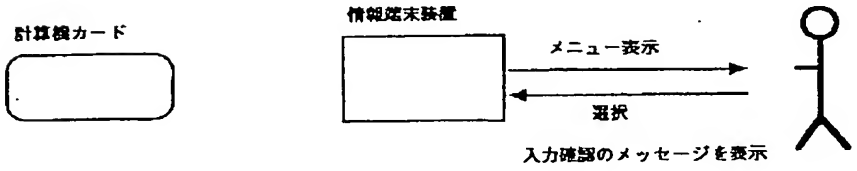
【図５】



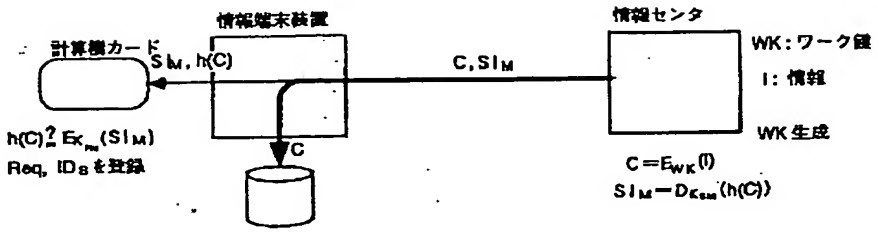
【図６】



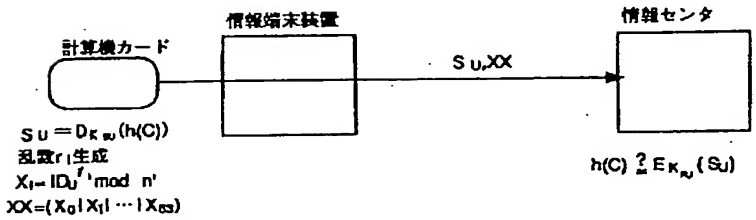
【図７】



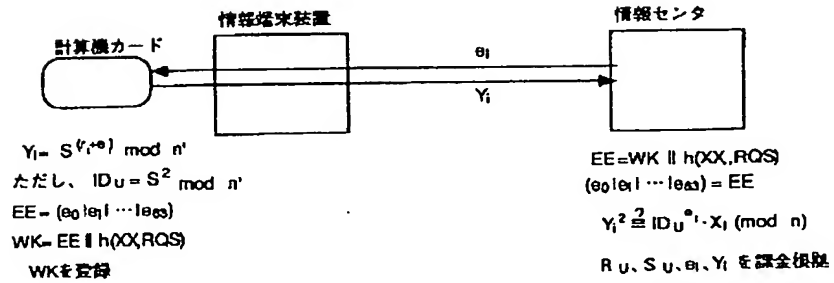
【図９】



【図１０】



【図１１】



【図１３】